УДК 351.74

Гордієнко Сергій Борисович
Кандидат технічних наук, доцент, завідувач кафедри Навчально-наукового інституту інформаційної безпеки
Національна академія Служби безпеки України, Київ
Манько Олександр Олексійович
Доктор технічних наук, професор
Одеська національна академія зв'язку ім. О.С. Попова, Одеса
Манько Володимир Олександрович
Кандидат технічних наук, інженер І категорії
Київстар GSM, Київ
Скубак Олександр Миколайович
Кандидат технічних наук, доцент, доцент кафедри Навчально-наукового інституту інформаційної безпеки
Національна академія Служби безпеки України, Київ

АНАЛІЗ ДОЦІЛЬНОСТІ РЕАЛІЗАЦІЇ ЗАХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *Розглянуто деякі аспекти прийняття рішень щодо управління інформаційною безпекою. За основу аналізу і подальшого прийняття рішень розглянуто економічний аналіз, який передбачає вивчення всіх факторів, під впливом яких відбувається розвиток аналізованих систем, закономірностей їх поведінки, динаміки зміни, а також використання універсальної грошової оцінки. Складність завдань економічного аналізу практично у всіх сферах діяльності, як правило, обумовлюється тим, що багато ключових параметрів економічних моделей неможливо достовірно оцінити. Як основний критерій здебільшого використовують функцію віддачі від інвестицій (ROI). Незважаючи на складні розрахунки згідно цієї моделі, пропонована методологія дає змогу менеджерам та спеціалістам у сфері засобів захисту інформації отримувати достовірні результати і правильно оцінювати ефективність засобів захисту інформації, а також визначати напрям їхнього розвитку.*

Ключові слова: інформаційна безпека; економічний аналіз; достовірність; засоби захисту; функція віддачі від інвестицій

Вступ

Управління інформаційною безпекою, так само як і управління в багатьох інших сферах діяльності, передбачає періодичне прийняття різних управлінських рішень, які полягають, як правило, у виборі певних альтернатив або визначенні деяких параметрів окремих організаційних і/або технічних систем і підсистем [1]. Одним з можливих підходів до вибору альтернатив в ситуації прийняття управлінського рішення є т. зв. "вольовий" підхід, коли рішення з тих чи інших причин приймається інтуїтивно і формально обґрунтований причинно-наслідковий взаємозв'язок між певними вихідними передумовами і конкретно прийнятим рішенням не може бути встановлений.

Очевидно, що альтернативою "вольовому" підходу стає прийняття рішень на підставі певних формальних процедур і послідовному аналізі.

Виклад основного матеріалу

Суть економічного аналізу в питаннях забезпечення інформаційної безпеки

Основою такого аналізу і подальшого прийняття рішень є економічний аналіз, який передбачає вивчення всіх факторів, під впливом яких відбувається розвиток аналізованих систем, закономірностей їх поведінки, динаміки зміни, а також використання універсальної грошової оцінки. Саме на основі адекватно побудованих економічних моделей і здійснюваного за їх допомогою економічного аналізу мають прийматися рішення, що стосуються як загальної стратегії розвитку, так і окремих організаційних і технічних заходів, як на рівні держав, регіонів і галузей, так і на рівні окремих підприємств, підрозділів і інформаційних систем.

При цьому так само, як і економіка будь-якої галузі діяльності, має свої особливості економіка інформаційної безпеки, що розглядається як відносно самостійна дисципліна, з одного боку, базується на

деяких загальних економічних законах і методах аналізу, а з іншого – потребує індивідуального розуміння, розвитку специфічних підходів до аналізу, накопиченні статистичних даних, специфічних для цієї сфери, формування стійких уявлень про чинники, під впливом яких функціонують інформаційні системи і засоби захисту інформації.

Складність завдань економічного аналізу практично у всіх сферах діяльності, як правило, обумовлюється тим, що багато ключових параметрів економічних моделей неможливо достовірно оцінити, оскільки вони носять імовірнісний характер. Аналіз ускладнюється також тим, що навіть невеликі коливання таких параметрів можуть серйозно вплинути на значення цільової функції і, відповідно, на рішення, що приймаються за результатами аналізу.

Отже, для забезпечення якомога більшої достовірності розрахунків у процесі проведення економічного аналізу і прийняття рішень необхідно організувати комплекс робіт зі збирання вихідної інформації, розрахунку прогнозних значень, з опитуванням експертів в різних сферах і опрацюванням всіх даних.

Особлива складність економічного аналізу у такій сфері, як інформаційна безпека, обумовлюється такими специфічними факторами:

– швидкий розвиток інформаційних технологій і методик, що використовуються в цій сфері (як засобів і методів захисту, так і засобів і методів нападу);

– неможливість достовірно передбачити всі можливі сценарії нападу на інформаційні системи і моделі поведінки нападників;

– неможливість дати достовірну, досить точну оцінку вартості інформаційних ресурсів, а також оцінити наслідки різних порушень в грошовому вимірі [1].

Це вимагає додаткових зусиль щодо організації процесу економічного аналізу, а також часто призводить до того, що багато прийнятих рішень, які стосуються забезпечення інформаційної безпеки, можуть виявитися неадекватними. Прикладами ситуацій, в яких недостатня розвиненість методології економічного аналізу негативно впливає на стан інформаційної безпеки, можуть бути випадки, коли:

– керівництво підприємства може прийняти неадекватні рішення щодо інвестицій в засоби захисту інформації, що, в свою чергу, може призвести до збитків, яких можна було б уникнути;

– керівництво підприємства може прийняти певні рішення щодо організації бізнес-процесів і процесів оброблення інформації на підприємстві, виходячи з прагнення скоротити поточні витрати і зменшити навантаження на персонал, при цьому не беручи до уваги економічні наслідки недостатньої захищеності інформаційних ресурсів;

– страхувальник і страховик можуть не укласти договір про страхування інформаційних ризиків або встановити неадекватні параметри такого договору з огляду на те, що відсутні моделі і методи оцінювання економічних параметрів угоди.

У процесі поточної діяльності підприємствам постійно доводиться стикатися з тими чи іншими змінами: уточнюються бізнес-процеси, змінюється кон'юнктура ринків збуту і ринків споживаних матеріальних ресурсів і послуг, з'являються нові технології, змінюють свою поведінку конкуренти і контрагенти, змінюється законодавство і політика держави та ін. У цих умовах менеджерам (в тому числі і керівникам, які відповідають за забезпечення інформаційної безпеки) доводиться постійно аналізувати зміни, що відбуваються і адаптувати свою роботу до постійно мінливої ситуації [2].

Конкретні форми, в яких проявляється реакція керівників, можуть бути різними. Це може бути зміна маркетингової політики, реорганізація бізнес-процесів, зміна технологій, зміна продукту, що виробляється, злиття з конкурентами або їх поглинання і т.п. Однак при всій різноманітності можливих моделей поведінки в мінливому середовищі майже всіх їх об'єднує один важливий загальний для них методологічний елемент: в більшості випадків реакція бізнесу на нові загрози і нові можливості передбачає здійснення нових більш-менш довгострокових і ресурсномістких вкладень (інвестицій) в певні організаційні та/або технічні заходи, які, з одного боку, припускають витрачання ресурсів (грошових коштів), а з іншого – дають можливість отримати нові вигоди, що виражаються в збільшенні доходу або скороченні деяких поточних витрат.

Отже, в ситуації, коли необхідно здійснити деякі нові організаційні або технічні заходи (реалізувати проект), основним завданням осіб, які відповідають за ефективну організацію інформаційної безпеки, є чітке співвіднесення витрат, які доведеться понести в зв'язку з реалізацією цього заходу, і додаткових (нових) грошових потоків, які будуть отримані. У даному випадку під грошовим потоком може розумітися економія витрат, запобігання збитків, а також додатковий дохід підприємства.

Як основний показник, що відображає це співвідношення, в економічній практиці прийнято використовувати функцію віддачі від інвестицій – Return on Investment *(ROI)* [4].

Отже, в цілому склад методології аналізу доцільності вкладень у проекти коштів, які спрямовані на забезпечення інформаційної безпеки, схематично показано на рисунку.

Рисунок – Структура методології аналізу ефективності вкладень у проекти щодо забезпечення інформаційної безпеки

Аналіз витрат, пов'язаних з реалізацією проекту, хоча і є відносно простішим завданням, все ж може викликати певні труднощі. Так само, як і для багатьох інших проектів у сфері інформаційних технологій, аналіз витрат на реалізацію проектів у сфері інформаційної безпеки доцільно здійснювати, використовуючи відому базову методологію "Total Cost of Ownership" – TCO (Сукупна вартість володіння – СВВ). Загалом ця методика орієнтована на забезпечення повноти аналізу витрат (як прямих, так і непрямих), пов'язаних з інформаційними технологіями та інформаційними системами; в ситуаціях, коли необхідно оцінити економічні наслідки впровадження та використання таких систем: при оцінці ефективності інвестицій, порівнянні альтернативних технологій, складанні капітальних і поточних бюджетів і т. п.

І хоча з математичної точки зору всі розрахунки в описаній рамковій моделі оцінювання *ROI* є гранично простими, визначення окремих параметрів (прогнозованих частоти порушень і розмірів втрат, а також передбачуваного терміну використання програмних і апаратних засобів і організаційних моделей) може викликати значні труднощі на практиці. Проведення таких розрахунків так само, як і проведення аудитів інформаційної безпеки, може зажадати залучення сторонніх консультантів. Однак кваліфікація і професійна спеціалізація таких консультантів може істотно відрізнятися від кваліфікації консультантів, що спеціалізуються, наприклад, на проведенні аудитів та впровадженні технічних засобів захисту інформації.

На сьогодні питання підбору кваліфікованих і досвідчених фахівців в галузі інформаційної безпеки, з огляду на економічну складову ефективного функціонування систем і технологій, забезпечення безпечної діяльності об`єктів критичної інформаційної інфраструктури, є найбільш актуальним і головним при побудові систем управління інформаційною безпекою на зазначених об`єктах.

Кваліфікований фахівець в галузі інформаційної безпеки в умовах сьогодення здатний забезпечити значний, прогнозований економічний ефект діяльності як державних структур, так і структур інших форм власності та сфер управління. Тому підготовці зазначених фахівців в державі приділяється багато уваги, що потребує значних капіталовкладень.

В Україні розробляються стандарти з безпеки для об'єктів критичної інфраструктури. Все частіше лунають заклики до більш активної взаємодії та обміну інформацією, а також до надання обов'язкової звітності про кібератаки та інші деструктивні впливи на інформаційні ресурси для спільної протидії та мінімізації наслідків таких атак. Слід очікувати визначення обов'язкових вимог у цій сфері. Навіть якщо це і не відбудеться в найближчому майбутньому, загальна атмосфера сьогодні така, що регулюючі органи, державні структури і навіть клієнти хочуть розширити свої знання про безпеку об'єктів інформаційної діяльності та збереження стратегічно важливих інформаційних ресурсів. Тому ми рекомендуємо шукати можливості для обміну інформацією та взаємодії з іншими суб'єктами діяльності у цій сфері для поліпшення стану інформаційної та кібербезпеки в Україні.

Враховуючи швидкість і складність сучасних кібератак та інших деструктивних впливів на державні, приватні, корпоративні ресурси, потрібне інвестування державних коштів у сферу інформаційної безпеки та кіберзахисту, яке гарантуватиме, по-перше, забезпечення на належному рівні національної безпеки, а по-друге – сталий економічний розвиток держави.

Причому, якщо оцінку ймовірностей атак, а також оцінку того, наскільки ці атаки можуть бути успішними, в переважній більшості можна довірити зовнішнім консультантам з інформаційної безпеки, то оцінку вартості інформації та економічних наслідків втрати контролю над інформаційними активами доцільно здійснювати самим фахівцям, які працюють на підприємстві (економістам, маркетологам і т.п.), а також залучати для цього сторонніх фахівців з відповідних сфер діяльності (маркетингу, фінансів, торгівлі і т.п.) [3].

Висновки

Незважаючи на всі труднощі процесу оцінювання доцільності впровадження засобів захисту, запропонована методологія дає змогу менеджерам і фахівцям із захисту інформації отримувати обгрунтовані оцінки і робити формалізовані висновки щодо того, наскільки виправданими є вкладення в певні засоби захисту інформації, а також визначити основні пріоритети

витрачання коштів, передбачених у бюджеті на забезпечення інформаційної безпеки (якщо підприємство практикує виділення фіксованих сум на ці цілі). При цьому досить високий рівень достовірності таких оцінок досягається за рахунок того, що вся робота з проведення оцінювання та підготовки інвестиційних рішень розкладається на кілька відносно більш простих і "прозорих" завдань, рішення кожного з яких може бути закріплено за фахівцями в певній сфері. В результаті загальна оцінка складається на основі отриманих рішень кількох окремих завдань, кожне з яких може бути проконтрольовано і за необхідності додатково уточнено.

У цих умовах загальна якість одержуваної аналітичної оцінки і відповідно формульованого рішення залежить від кваліфікації всіх експертів, аналітиків і фахівців, що беруть участь в роботі. Тож, одним з основних завдань керівників підприємства і менеджерів, які відповідають за забезпечення інформаційної безпеки і прийняття рішень в цій сфері, є підбір найбільш кваліфікованих і досвідчених фахівців, оскільки від якості їх роботи буде залежати не просто безпека окремих елементів інформаційних активів у певні моменти часу, а ефективність всієї системи захисту інформації в середньостроковій, а іноді і в довгостроковій перспективі.

Список літератури

1. *Анисимов А.А. Менеджмент в сфере информационной безопасности / А.А. Анисимов. – М.: БИНОМ, 2009.*
2. *Курило А.П., Милославская Н.Г., Сенаторов М.Ю. и др. Основи управления информационной безопасностью / А.П. Курило, Н.Г. Милославская., М.Ю. Сенаторов и др. – М.: Горячая линия-Телеком, 2012.*
3. *Петренко, С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи, ДМК-Пресс, 2004.*
4. *Артемов В.Ю. Основи менеджменту для інформаційних аналітиків: Курс лекцій. / В.Ю. Артемов – К.: КНТ, 2007.*
5. *Домарев, В. В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В. В. Домарєв, В. В. Домарєв. – Донецьк : Велстар, 2012, 2012 – 146 с.*
6. *Милославская Н.Г., Сенаторов М. Ю., Толстой А. П. Управление инцидентами информационной безопасности и непрерывностью бизнеса. – М.: Горячая линия-Телеком, 2014. – 170 с.*
7. *Милославская Н.Г., Сенаторов М. Ю., Толстой А. П. Управление рисками информационной безопасности. – М.: Горячая линия-Телеком, 2013. – 130 с.*
8. *ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)*
9. *ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).*
10. *ДСТУ ISO/IEC 27005:2015. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).*
11. *ДСТУ ISO/IEC 27006:2015. Інформаційні технології. Методи захисту. Вимоги до організацій, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2011, IDT).*
12. *Гордієнко С.Б. Перспективи розвитку сучасних мереж доступу / С.Б. Гордієнко, О.О. Манько, В.О. Манько, О.М. Скубак / //Управління розвитком складних систем. – 2018. – № 33. – С. 122 – 129.*

Стаття надійшла до редколегії 10.10.2018

Рецензент: д-р техн. наук, В.В. Онищенко, Державний університет телекомунікацій, Київ.

Гордиенко Сергей Борисович
Кандидат технических наук, доцент, заведующий кафедрой Учебно-научного института информационной безопасности
Национальная академия Службы безопасности Украины, Киев
Манько Александр Алексеевич
Доктор технических наук, профессор
Одесская национальная академия связи им. А.С. Попова, *Одесса*
Манько Владимир Александрович
Кандидат технических наук, инженер I категории,
Киевстар GSM, Киев
Скубак Александр Николаевич
Кандидат технических наук, доцент, доцент Учебно-научного института информационной безопасности
Национальная академия Службы безопасности Украины, Киев

АНАЛИЗ ЦЕЛЕСООБРАЗНОСТИ РЕАЛИЗАЦИИ СРЕДСТВ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *Рассмотрен ряд аспектов принятия решений по управлению информационной безопасностью. В качестве основы для анализа и дальнейшего принятия решений рассматривается экономический анализ. Сложность задач экономического анализа связана с тем, что многие ключевые параметры экономических моделей не могут быть достоверно оценены. В качестве основного критерия принято использовать функцию возврата инвестиций (ROI). Несмотря на сложные расчеты по этой модели, предлагаемая методология позволяет менеджерам и специалистам в области средств информационной безопасности получать достоверные результаты и правильно оценивать эффективность средств защиты информации, а также определять направление их развития.*

Ключевые слова: информационная безопасность; экономический анализ; достоверность; средства защиты; функция отдачи от инвестиций

Gordienko Sergey Borisovich
PhD (Eng.), Associate Professor, Associate Professor of the Educational and Scientific Institute of Information Security
National Academy of Security Service of Ukraine, Kyiv
Manko Alexander Alexeyevich
DSc (Eng.), Professor of Odessa National Academy of Telecommunications named O.S. Popov
Odessa National Academy of Telecommunications named O.S. Popov, Kyiv
Manko Vladimir Alexandrovich
PhD (Eng.), engineer of the 1-st category,
Joint-stock company Kyivstar GSM, Kyiv
Skubak Alexander Nikolaevich
PhD (Eng.) Associate Professor, Associate Professor of the Educational and Scientific Institute of Information Security
National Academy of Security Service of Ukraine, Kyiv

ANALYSIS OF ADVISABILITY OF IMPLEMENTATION OF MEANS TO ENSURE INFORMATION SECURITY

Abstract. *In this paper, some aspects of decision-making on information security management are considered. As a basis for analysis and further decision-making, economic analysis is considered. The complexity of the tasks of economic analysis is due to the fact that many key parameters of economic models can not be reliably estimated. To ensure greater reliability of calculations in the process of economic analysis, it is necessary to organize a set of work to collect output information. The special complexity of economic analysis in such a sphere as information security is conditioned by such specific factors: rapid development of information and related technologies; the inability to reliably provide all possible scenarios and models of attacks on information systems; the inability to provide a fairly accurate estimate of the cost of information resources and assess the consequences of violations. This requires additional efforts to organize the process of economic analysis. In the course of current activity, enterprises have to constantly face a number of changing factors. The specific forms in which the actions of the manager are manifested may be different. Thus, in a critical situation, there is a need for a clear correlation of costs and benefits during the execution of safety work. As the main criterion, it is customary to use the return on investment (ROI) function. In this case, calculations according to this model can meet considerable difficulties in practice. At the same time, the proposed methodology allows managers and specialists in information security tools to obtain valid results and to make a proper assessment of the effectiveness of information protection tools and also determine the direction of their development.*

Key words: information security, economic analysis, reliability, means of protection, return on investment function

References

1. Anisimov, A.A. (2009). Management in the field of information security. Moscow, Russia: BINOM.

2. Kurilo, A.P., Miloslavskaya, N.G., Senatorov, M.Yu. (2012). The basis of information security. Moscow, Russia: Hot line-Telecom.

3. Petrenko, S.A. Simonov, S.V. (2004). Information Risk Management. Economically justified safety Moscow, Russia: IT Co., DMK-Press.

4. Artemov, V.Yu. (2007). Fundamentals of Management for Information Analysts: Course of lectures. Kyiv, Ukraine: KNT.

5. Domarev, V.V. (2012). Management of Information Security in Banking Institutions (Theory and Practice of Implementation of ISO 27k Standards). Donetsk: Velstar, 146.

6. Miloslavskaya, N.G., Senatorov, M. Yu., Tolstoy, A.P. (2014). Management of incidents of information security and business continuity. Moscow, Russia: Hot line-Telecom, 170.

7. Miloslavskaya, N.G., Senatorov, M. Yu., Tolstoy, A.P. (2013). Information Security Risk Management. Moscow, Russia: Hot line-Telecom, 130.

8. DSTU ISO / IEC 27001: 2015. Information Technology. Methods of protection. Information Security Management Systems. Requirements (ISO / IEC 27001: 2013; Cor 1: 2014, IDT).

9. DSTU ISO / IEC 27002: 2015. Information Technology. Methods of protection. A set of practices on information security measures (ISO / IEC 27002: 2013; Cor 1: 2014, IDT).

10. DSTU ISO / IEC 27005: 2015. Information Technology. Methods of protection. Information Security Risk Management (ISO / IEC 27005: 2011, IDT).

11. DSTU ISO / IEC 27006: 2015. Information Technology. Methods of protection. Requirements for organizations providing audit and certification services for information security management systems (ISO / IEC 27006: 2011, IDT).

12. Gordienko, Sergij, Manko, Olexandr, Manko, Volodimir, Skubak, Olexandr & Tverdokhleb, Nikolay. (2018). Perspectives of the development of modern access networks. Management of Development of Complex Systems, (33), 122-129.

Посилання на публікацію

APA *Gordienko, Sergij, Manko, Olexandr, Manko, Volodimir & Skubak, Olexandr. (2018). Analysis of advisability of implementation of means. Management of Development of Complex Systems, 36, 89 – 94.*

ДСТУ *Гордієнко С.Б. Аналіз доцільності реалізації заходів щодо забезпечення інформаційної безпеки [Текст] / С.Б. Гордієнко, О.О. Манько, В.О. Манько, О.М., О.М. Скубак // Управління розвитком складних систем. – 2018. – № 36. – С. 89 – 94.*